BULLETIN (SB19-119)
VULNERABILITY SUMMARY FOR THE WEEK OF
APRIL 22, 2019

CYBERNETIC
GLOBAL INTELLIGENCE
Run Your Business. We'll Protect It .

Bulletin (SB19-119)
Vulnerability Summary for the Week of April 22, 2019

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium and low severities correspond to the following scores:

High - Vulnerabilities will be labeled High severity if they have a CVSS base score of 10.0 - 7.0

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of - 4.0 6.9

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 3.9 - 0.0

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Source references taken from US-CERT

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activision -- call_of_duty:_advanced_warfare	SV_SteamAuthClient in various Activision Infinity Ward Call of Duty games before 2015-08-11 is missing a size check when reading authBlob data into a buffer, which allows one to execute code on the remote target machine when sending a steam authentication request. This affects Call of Duty: Modern Warfare 2, Call of Duty: Modern Warfare 3, Call of Duty: Ghosts, Call of Duty: Advanced Warfare, Call of Duty: Black Ops 1, and Call of Duty: Black Ops 2.	2019-04-19	7.5	CVE-2018-20817 MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. The Number#toFixed() and numtostr implementations in jsnumber.c have a stack-based buffer overflow.	2019-04-22	7.5	CVE-2019-11411 MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. A remote attacker may send a crafted packet triggering a stack-based buffer overflow due to an insecurely implemented strncpy call. The vulnerability is triggered by sending an error packet of 3 bytes or fewer. There are multiple instances of this vulnerable strncpy pattern within the code base, specifically within tftpd_file.c, tftp_file.c, tftpd_mtftp.c, and tftp_mtftp.c.	2019-04-20	7.5	CVE-2019-11365 MISC MISC
burrow-wheeler_aligner_project -- burrow-wheeler_aligner	BWA (aka Burrow-Wheeler Aligner) 0.7.17 r1198 has a Buffer Overflow via a long prefix that is mishandled in bns_fasta2bntseq and bns_dump at btnseq.c.	2019-04-20	7.5	CVE-2019-11371 MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a “Dragonblood” issue, a similar issue to CVE-2019-9497.	2019-04-22	7.5	CVE-2019-11234 CONFIRM MISC MISC MISC UBUNTU MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 mishandles the “each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used” protection mechanism, aka a “Dragonblood” issue, a similar issue to CVE-2019-9498 and CVE-2019-9499.	2019-04-22	7.5	CVE-2019-11235 CONFIRM MISC MISC MISC UBUNTU MISC
google -- android	In floor0_inverse1 of floor0.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119120561.	2019-04-19	9.3	CVE-2019-2027 CONFIRM
google -- android	In numerous hand-crafted functions in libmpeg2, NEON registers are not preserved. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120644655.	2019-04-19	9.3	CVE-2019-2028 CONFIRM
google -- android	In removeInterfaceAddress of NetworkController.cpp, there is a possible use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119496789.	2019-04-19	7.5	CVE-2019-2030 CONFIRM
ibm -- bladecenter_hs23_firmware	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service.	2019-04-22	7.8	CVE-2019-6155 MISC
imagemagick -- imagemagick	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.	2019-04-23	7.1	CVE-2019-11470 MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. A malformed login request allows remote attackers to cause a denial of service (reboot), as demonstrated by JSON misparsing of the \""} string to v1/system/login.	2019-04-22	7.8	CVE-2019-11415 MISC
intelbras -- iwr_3000n_firmware	A CSRF issue was discovered on Intelbras IWR 3000N 1.5.0 devices, leading to complete control of the router, as demonstrated by v1/system/user.	2019-04-22	9.3	CVE-2019-11416 MISC
linux -- linux_kernel	cipso_v4_validate in include/net/cipso_ipv4.h in the Linux kernel before 3.11.7, when CONFIG_NETLABEL is disabled, allows attackers to cause a denial of service (infinite loop and crash), as demonstrated by icmpsic, a different vulnerability than CVE-2013-0310.	2019-04-22	7.1	CVE-2013-7470 MISC MISC MISC
mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the login interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	CVE-2018-18285 CONFIRM CONFIRM

mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the changepwd interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	CVE-2018-18286 CONFIRM CONFIRM
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	CVE-2019-9788 MISC MISC MISC MISC
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 66.	2019-04-26	7.5	CVE-2019-9789 MISC MISC
mozilla -- firefox	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	CVE-2019-9790 MISC MISC MISC MISC
mozilla -- thunderbird	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	CVE-2018-18512 MISC MISC
neatorobotics -- botvac_connected_firmware	A Buffer Overflow in Network::AuthenticationClient::VerifySignature in /bin/astro in Neato Botvac Connected 2.2.0 allows a remote attacker to execute arbitrary code with root privileges via a crafted POST request to a nucleo.neatocloud.com:4443/vendors/neato/robots/[robot_serial]/messages Neato cloud URL.	2019-04-25	10.0	CVE-2018-19442 MISC
nice -- engage	In NICE Engage through 6.5, the default configuration binds an unauthenticated JMX/RMI interface to all network interfaces, without restricting registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol by using the JMX connector. The observed affected TCP port is 6338 but, based on the product's configuration, a different one could be vulnerable.	2019-04-23	7.5	CVE-2019-7727 FULLDISC MISC BUGTRAQ
nmap -- npcap	An issue was discovered in Npcap 0.992. Sending a malformed .pcap file with the loopback adapter using either pcap_sendqueue_queue() or pcap_sendqueue_transmit() results in kernel pool corruption. This could lead to arbitrary code executing inside the Windows kernel and allow escalation of privileges.	2019-04-23	9.3	CVE-2019-11490 MISC
openkm -- openkm	OpenKM 6.3.2 through 6.3.7 allows an attacker to upload a malicious JSP file into the /okm:root directories and move that file to the home directory of the site, via frontend/FileUpload and admin/repository_export.jsp. This is achieved by interfering with the Filesystem path control in the admin's Export field. As a result, attackers can gain remote code execution through the application server with root privileges.	2019-04-22	9.0	CVE-2019-11445 MISC MISC
openplcproject -- openplc_v2_firmware	A buffer overflow vulnerability was discovered in the OpenPLC controller, in the OpenPLC_v2 and OpenPLC_v3 versions. It occurs in the modbus.cpp mapUnusedIO() function, which can cause a runtime crash of the PLC or possibly have unspecified other impact.	2019-04-22	7.5	CVE-2018-20818 MISC
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having DBFS_ROLE privilege with network access via Oracle Net to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	7.5	CVE-2019-2517 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	CVE-2019-2608 MISC

oracle -- retail_convenience_store_back_office	Vulnerability in the Oracle Retail Convenience Store Back Office component of Oracle Retail Applications (subcomponent: Level 3 Maintenance Functions). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Convenience Store Back Office. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Convenience Store Back Office accessible data as well as unauthorized read access to a subset of Oracle Retail Convenience Store Back Office accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Convenience Store Back Office. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	CVE-2019-2424 MISC
oracle -- retail_point-of-service	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: Infrastructure). Supported versions that are affected are 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Point-of-Service accessible data as well as unauthorized read access to a subset of Oracle Retail Point-of-Service accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Point-of-Service. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	CVE-2019-2558 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	CVE-2019-2645 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	CVE-2019-2646 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	CVE-2019-2658 MISC
pluck-cms -- pluck	data/inc/files.php in Pluck 4.7.8 allows remote attackers to execute arbitrary code by uploading a .htaccess file that specifies SetHandler x-httpd-php for a .txt file, because only certain PHP-related filename extensions are blocked.	2019-04-19	7.5	CVE-2019-11344 MISC
rocboss -- rocboss	app/controllers/frontend/PostController.php in ROCBOSS V2.2.1 has SQL injection via the Post:doReward score paramter, as demonstrated by the /do/reward/3 URI.	2019-04-20	7.5	CVE-2019-11362 MISC
tabslab -- mailcarrier	A buffer overflow in MailCarrier 2.51 allows remote attackers to execute arbitrary code via a long string, as demonstrated by SMTP RCPT TO, POP3 USER, POP3 LIST, POP3 TOP, or POP3 RETR.	2019-04-22	7.5	CVE-2019-11395 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
trendnet -- tew-632brp_firmware	apply.cgi on the TRENDnet TEW-632BRP 1.010B32 router has a buffer overflow via long strings to the SOAPACTION:HNAP1 interface.	2019-04-22	7.5	CVE-2019-11418 MISC
trendnet -- tv-ip110wn_firmware	system.cgi on TRENDnet TV-IP110WN cameras has a buffer overflow caused by an inadequate source-length check before a strcpy operation in the respondAsp function. Attackers can exploit the vulnerability by using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68.	2019-04-22	7.5	CVE-2019-11417 MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?question/ajaxadd.html title SQL injection.	2019-04-22	7.5	CVE-2019-11450 MISC

zohocorp -- manageengine_applications_manager	An issue was discovered in Zoho ManageEngine Applications Manager 11.0 through 14.0. An unauthenticated user can gain the authority of SYSTEM on the server due to a Popup_SLA.jsp sid SQL injection vulnerability. For example, the attacker can subsequently write arbitrary text to a .vbs file.	2019-04-22	10.0	CVE-2019-11448 MISC MISC MISC EXPLOIT-DB CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
74cms -- 74cms	74CMS v5.0.1 has a CSRF vulnerability to add a new admin user via the index.php?m=Admin&c=admin&a=add URI.	2019-04-20	6.8	CVE-2019-11374 MISC MISC EXPLOIT-DB
apache -- pony_mail	A vulnerability was discovered wherein a specially crafted URL could enable reflected XSS via JavaScript in the pony mail interface.	2019-04-22	4.3	CVE-2019-0218 BID MLIST MLIST
apache -- zeppelin	Apache Zeppelin prior to 0.8.0 had a stored XSS issue via Note permissions. Issue reported by "Josna Joseph".	2019-04-23	4.3	CVE-2018-1328 MLIST BID MLIST MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 allows Information Exposure through Log Files because of an error in the Log-File writer component.	2019-04-24	5.0	CVE-2019-9724 CONFIRM MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. jscompile.c can cause a denial of service (invalid stack-frame jump) because it lacks an ENDTRY opcode call.	2019-04-22	5.0	CVE-2019-11412 MISC MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. It has unlimited recursion because the match function in regexp.c lacks a depth check.	2019-04-22	5.0	CVE-2019-11413 MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftpd_list.c check, there is a crash when dereferencing current->next.	2019-04-20	4.3	CVE-2019-11366 MISC MISC
atutor -- atutor	An issue was discovered in ATutor through 2.2.4. It allows the user to run commands on the server with the teacher user privilege. The Upload Files section in the File Manager field contains an arbitrary file upload vulnerability via upload.php. The $IllegalExtensions value only lists lowercase (and thus .phP is a bypass), and omits .shtml and .phtml.	2019-04-22	6.5	CVE-2019-11446 MISC EXPLOIT-DB
audiocodes -- 405hd_firmware	Cross Site Scripting in different input fields (domain field and personal settings) in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an attacker (local or remote) to inject JavaScript into the web interface of the device by manipulating the phone book entries or manipulating the domain name sent to the device from the domain controller.	2019-04-25	4.3	CVE-2018-16220 MISC
block -- jit-wasm	EOS.IO jit-wasm 4.1 has a heap-based buffer overflow via a crafted wast file.	2019-04-24	6.8	CVE-2018-13443 MISC MISC MISC
brassica -- soy_cms	** DISPUTED ** SOY CMS v3.0.2 allows remote attackers to execute arbitrary PHP code via a <?php substring in the second text box. NOTE: the vendor indicates that there was an assumption that the content is "made editable on its own."	2019-04-20	6.5	CVE-2019-11376 MISC MISC
cloudbees -- jenkins_operations_center	CloudBees Jenkins Operations Center 2.150.2.3, when an expired trial license exists, allows Cleartext Password Storage and Retrieval via the proxy configuration page.	2019-04-19	5.0	CVE-2019-11350 MISC
cutephp -- cutenews	An issue was discovered in CutePHP CuteNews 2.1.2. An attacker can infiltrate the server through the avatar upload process in the profile area via the avatar_file field to index.php?mod=main&opt=personal. There is no effective control of $imgsize in /core/modules/dashboard.php. The header content of a file can be changed and the control can be bypassed for code execution. (An attacker can use the GIF header for this.)	2019-04-22	6.5	CVE-2019-11447 MISC EXPLOIT-DB
datools -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed DIB format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9135 MISC

datools -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed JPEG2000 format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9136 MISC
datools -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PhotoShop file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9138 MISC
datools -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PDF file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9139 MISC
dropbox -- lepton	read_ujpg in jpgcoder.cc in Dropbox Lepton 1.2.1 allows attackers to cause a denial-of-service (application runtime crash because of an integer overflow) via a crafted file.	2019-04-23	4.3	CVE-2018-20820 MISC MISC
drupal -- drupal	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object. prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	2019-04-19	4.3	CVE-2019-11358 BID MISC MISC MISC MISC MLIST MLIST MLIST MLIST MLIST BUGTRAQ MISC DEBIAN MISC
ea -- origin	The client in Electronic Arts (EA) Origin 10.5.36 on Windows allows template injection in the title parameter of the Origin2 URI handler. This can be used to escape the underlying AngularJS sandbox and achieve remote code execution via an origin2://game/launch URL for QtApplication QDesktopServices communication.	2019-04-19	6.8	CVE-2019-11354 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
eclipse -- jetty	In Eclipse Jetty version 9.2.26 and older, 9.3.25 and older, and 9.4.15 and older, the server is vulnerable to XSS conditions if a remote client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is configured for showing a Listing of directory contents.	2019-04-22	4.3	CVE-2019-10241 CONFIRM
fortinet -- fortimanager	A cleartext transmission of sensitive information vulnerability in Fortinet FortiManager 5.2.0 through 5.2.7, 5.4.0 and 5.4.1 may allow an unauthenticated attacker in a man in the middle position to retrieve the admin password via intercepting REST API JSON responses.	2019-04-25	4.3	CVE-2018-1360 BID CONFIRM
gilacms -- gila_cms	Gila CMS 1.10.1 allows fm/save CSRF for executing arbitrary PHP code.	2019-04-22	6.8	CVE-2019-11456 MISC
gilacms -- gila_cms	core/classes/db_backup.php in Gila CMS 1.10.1 allows admin/db_backup?download= absolute path traversal to read arbitrary files.	2019-04-25	4.0	CVE-2019-11515 MISC
gitlab -- gitlab	GitLab CE & EE 11.2 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 have Persistent XSS.	2019-04-25	4.3	CVE-2018-18643 MISC MISC MISC
gitlab -- gitlab	GitLab Community and Enterprise Edition 8.9 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 has Incorrect Access Control.	2019-04-25	6.5	CVE-2018-19359 MISC MISC MISC
gnome -- evince	The tiff_document_render() and tiff_document_get_thumbnail() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBAImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.	2019-04-22	4.3	CVE-2019-11459 MISC
gnome -- gnome-desktop	An issue was discovered in GNOME gnome-desktop 3.26, 3.28, and 3.30 prior to 3.30.2.2, and 3.32 prior to 3.32.1.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	6.8	CVE-2019-11460 MISC

google -- android	In updateAssistMenuItems of Editor.java, there is a possible escape from the Setup Wizard due to a missing permission check. This could lead to local escalation of privilege and FRP bypass with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0Android ID: A-120866126	2019-04-19	4.6	CVE-2019-2026 CONFIRM
google -- android	In btm_proc_smp_cback of tm_ble.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120612744.	2019-04-19	6.8	CVE-2019-2029 CONFIRM
google -- android	In rw_t3t_act_handle_check_ndef_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120502559.	2019-04-19	4.6	CVE-2019-2031 CONFIRM
google -- android	In SetScanResponseData of ble_advertiser_hci_interface.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-121145627.	2019-04-19	4.6	CVE-2019-2032 CONFIRM
google -- android	In create_hdr of dnssd_clientstub.c, there is a possible use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-121327565.	2019-04-19	4.6	CVE-2019-2033 CONFIRM
google -- android	In rw_i93_sm_read_ndef of rw_i93.cc, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the NFC process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122035770.	2019-04-19	6.8	CVE-2019-2034 CONFIRM
google -- android	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122320256	2019-04-19	6.8	CVE-2019-2035 CONFIRM
google -- android	In l2cu_send_peer_config_rej of l2c_utils.cc, there is a possible out-of-bound read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119870451.	2019-04-19	5.0	CVE-2019-2037 CONFIRM
google -- android	In rw_i93_process_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121259048.	2019-04-19	4.3	CVE-2019-2038 CONFIRM
google -- android	In rw_i93_sm_detect_ndef of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121260197.	2019-04-19	4.7	CVE-2019-2039 CONFIRM
google -- android	In rw_i93_process_ext_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122316913.	2019-04-19	4.7	CVE-2019-2040 CONFIRM
google -- android	In the configuration of NFC modules on certain devices, there is a possible failure to distinguish individual devices due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.1 Android-9. Android ID: A-122034690.	2019-04-19	6.9	CVE-2019-2041 CONFIRM
google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by: Null Pointer Dereference. The type of exploitation is: context-dependent.	2019-04-23	4.3	CVE-2018-7576 CONFIRM
google -- tensorflow	Google TensorFlow 1.7 and below is affected by: Buffer Overflow. The impact is: execute arbitrary code (local).	2019-04-23	6.8	CVE-2018-8825 CONFIRM
google -- tensorflow	NULL pointer dereference in Google TensorFlow before 1.12.2 could cause a denial of service via an invalid GIF file.	2019-04-24	4.3	CVE-2019-9635 MISC
gradle -- enterprise	In Gradle Enterprise before 2018.5.3, Build Cache Nodes did not store the credentials at rest in an encrypted format.	2019-04-22	5.0	CVE-2019-11402 MISC

gradle -- enterprise	In Gradle Enterprise before 2018.5.2, Build Cache Nodes would reflect the configured password back when viewing the HTML page source of the settings page.	2019-04-22	5.0	CVE-2019-11403 MISC
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (out-of-bounds read and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11473 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (floating-point exception and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11474 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.8 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WritePDBImage of coders/pdb.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to MagickBitStreamMSBWrite in magick/bit_stream.c.	2019-04-24	6.8	CVE-2019-11505 MISC BID MISC
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.30 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WriteMATLABImage of coders/mat.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to ExportRedQuantumType in magick/export.c.	2019-04-24	6.8	CVE-2019-11506 MISC MISC
gstreamer_project -- gstreamer	GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution.	2019-04-24	6.8	CVE-2019-9928 CONFIRM CONFIRM MLIST MLIST
i-librarian -- i,_librarian	Cross-site scripting (XSS) vulnerability in display.php in I, Librarian 4.10 allows remote attackers to inject arbitrary web script or HTML via the project parameter.	2019-04-19	4.3	CVE-2019-11359 MISC
i-librarian -- i,_librarian	I, Librarian 4.10 has XSS via the export.php export_files parameter.	2019-04-22	4.3	CVE-2019-11428 MISC
i-librarian -- i,_librarian	I, Librarian 4.10 has XSS via the notes.php notes parameter.	2019-04-22	4.3	CVE-2019-11449 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 157654.	2019-04-25	5.8	CVE-2019-4092 CONFIRM XF
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 147708.	2019-04-19	5.0	CVE-2018-1729 CONFIRM BID XF
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to view process definition of a business process without permission. IBM X-Force ID: 159231.	2019-04-25	4.0	CVE-2019-4222 XF CONFIRM
idreamsoft -- icms	An XSS issue was discovered in app/admincp/template/admincp.header.php in idreamsoft iCMS 7.0.14 via the admincp.php?app=config tab parameter.	2019-04-22	4.3	CVE-2019-11426 MISC
idreamsoft -- icms	An XSS issue was discovered in app/search/search.app.php in idreamsoft iCMS 7.0.14 via the public/api.php?app=search q parameter.	2019-04-22	4.3	CVE-2019-11427 MISC
imagemagick -- imagemagick	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.	2019-04-23	4.3	CVE-2019-11472 MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. When the administrator password is changed from a certain client IP address, administrative authorization remains available to any client at that IP address, leading to complete control of the router.	2019-04-22	4.3	CVE-2019-11414 MISC
kubernetes -- kubernetes	In Kubernetes v1.12.0-v1.12.4 and v1.13.0, the rest.AnonymousClientConfig() method returns a copy of the provided config, with credentials removed (bearer token, username/password, and client certificate/key data). In the affected versions, rest.AnonymousClientConfig() did not effectively clear service account credentials loaded using rest.InClusterConfig()	2019-04-22	4.3	CVE-2019-11243 BID MISC

linux -- linux_kernel	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	2019-04-23	6.9	CVE-2019-11486 MISC MISC MISC MISC MISC MISC
matrix -- sydent	util/emailutils.py in Matrix Sydent before 1.0.2 mishandles registration restrictions that are based on e-mail domain, if the allowed_local_3pids option is enabled. This occurs because of potentially unwanted behavior in Python, in which an email.utils.parseaddr call on user@bad.example.net@good.example.com returns the user@bad.example.net substring.	2019-04-19	4.3	CVE-2019-11340 MISC MISC MISC MISC
mediaarea -- mediainfo	An out-of-bounds read in MediaInfoLib::File__Tags_Helper::Synched_Test in Tag/File__Tags.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11372 MISC FEDORA MISC
mediaarea -- mediainfo	An out-of-bounds read in File__Analyze::Get_L8 in File__Analyze_Buffer.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11373 MISC FEDORA MISC
meisivod -- msvod	Msvod v10 has a CSRF vulnerability to change user information via the admin/member/edit.html URI.	2019-04-20	4.3	CVE-2019-11375 MISC MISC EXPLOIT-DB
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11387 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11388 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with next# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11389 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with set_error_handler# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11390 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with $a# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11391 MISC
mozilla -- firefox	The about:crashcontent and about:crashparent pages can be triggered by web content. These pages are used to crash the loaded page or the browser for test purposes. This issue allows for a non-persistent denial of service (DOS) attack by a malicious site which links to these pages. This vulnerability affects Firefox < 64.	2019-04-26	4.3	CVE-2018-18510 MISC MISC
openstack -- nova	Versions of nova before 2012.1 could expose hypervisor host files to a guest operating system when processing a maliciously constructed qcow filesystem.	2019-04-22	5.0	CVE-2011-3147 MISC
oracle -- advanced_outbound_telephony	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2663 MISC

oracle -- application_object_library	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2621 MISC
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	CVE-2019-2557 MISC
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2682 MISC
oracle -- autovue_3d_professional_advanced	Vulnerability in the Oracle AutoVue 3D Professional Advanced component of Oracle Supply Chain Products Suite (subcomponent: Format Handling - 2D). Supported versions that are affected are 21.0.0 and 21.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue 3D Professional Advanced. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle AutoVue 3D Professional Advanced accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	CVE-2019-2575 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.0	CVE-2019-2588 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2595 MISC

oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	4.9	CVE-2019-2601 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2019-04-23	6.4	CVE-2019-2616 MISC
oracle -- business_process_management_suite	Vulnerability in the Oracle Business Process Management Suite component of Oracle Fusion Middleware (subcomponent: BPM Foundation Services). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Process Management Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Process Management Suite accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2706 MISC BID
oracle -- commerce_merchandising	Vulnerability in the Oracle Commerce Merchandising component of Oracle Commerce (subcomponent: Asset Manager). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Merchandising. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Merchandising accessible data as well as unauthorized read access to a subset of Oracle Commerce Merchandising accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-04-23	6.4	CVE-2019-2713 MISC
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2659 MISC
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). Supported versions that are affected are 11.2.0.3 and 11.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2712 MISC

oracle -- common_applications	Vulnerability in the Oracle Common Applications component of Oracle E-Business Suite (subcomponent: CRM User Management Framework). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2665 MISC
oracle -- configurator	Vulnerability in the Oracle Configurator component of Oracle Supply Chain Products Suite (subcomponent: Active Model Generation). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2567 MISC
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2639 MISC
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2669 MISC
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2669 MISC
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2671 MISC

oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2675 MISC
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2676 MISC
oracle -- database	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2619 MISC
oracle -- database_server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2516 MISC
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	CVE-2019-2518 MISC
oracle -- database_server	Vulnerability in the RDBMS DataPump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Difficult to exploit vulnerability allows high privileged attacker having DBA role privilege with network access via Oracle Net to compromise RDBMS DataPump. Successful attacks of this vulnerability can result in takeover of RDBMS DataPump. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	CVE-2019-2571 MISC
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	CVE-2019-2582 MISC
oracle -- e-business_suite	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2551 MISC

oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2600 MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2651 MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2661 MISC
oracle -- general_ledger	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	CVE-2019-2638 MISC
oracle -- health_sciences_data_management_workbench	Vulnerability in the Oracle Health Sciences Data Management Workbench component of Oracle Health Sciences Applications (subcomponent: User Interface). The supported version that is affected is 2.4.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences Data Management Workbench accessible data as well as unauthorized read access to a subset of Oracle Health Sciences Data Management Workbench accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2019-04-23	5.5	CVE-2019-2629 MISC
oracle -- hospitality_cruise_dining_room_management	Vulnerability in the Oracle Hospitality Cruise Dining Room Management component of Oracle Hospitality Applications (subcomponent: Web Service). The supported version that is affected is 8.0.80. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Dining Room Management. While the vulnerability is in Oracle Hospitality Cruise Dining Room Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room Management accessible data. CVSS 3.0 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2019-04-23	6.4	CVE-2019-2702 MISC

oracle -- interaction_center_ intelligence	Vulnerability in the Oracle Interaction Center Intelligence component of Oracle E-Business Suite (subcomponent: Business Intelligence (OLTP)). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Interaction Center Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Interaction Center Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Interaction Center Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Interaction Center Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2655 MISC
oracle -- istore	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2652 MISC
oracle -- isupplier_portal	Vulnerability in the Oracle iSupplier Portal component of Oracle E-Business Suite (subcomponent: Attachments). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupplier Portal, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupplier Portal accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2583 MISC
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2564 MISC
oracle -- jd_edwards_world_technical_foundation	Vulnerability in the JD Edwards World Technical Foundation component of Oracle JD Edwards Products (subcomponent: Service Enablement). Supported versions that are affected are A9.2, A9.3.1 and A9.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards World Technical Foundation. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards World Technical Foundation accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2565 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	5.0	CVE-2019-2602 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2019-04-23	4.3	CVE-2019-2684 MISC

oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2697 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2698 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). The supported version that is affected is Java SE: 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2699 MISC CONFIRM
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: Setup, Admin). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2660 MISC
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge component of Oracle Siebel CRM (subcomponent: Web Applications (InfoCenter)). Supported versions that are affected are 8.5.1.0 - 8.5.1.7, 8.6.0 and 8.6.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data as well as unauthorized read access to a subset of Oracle Knowledge accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2719 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2604 MISC

oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2664 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2670 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2673 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2677 MISC
oracle -- micros_lucas	Vulnerability in the MICROS Lucas component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 2.9.5.6 and 2.9.5.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Lucas. Successful attacks of this vulnerability can result in takeover of MICROS Lucas. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	CVE-2018-3120 MISC
oracle -- micros_relate_customer_relationship_management_software	Vulnerability in the MICROS Relate CRM Software component of Oracle Retail Applications (subcomponent: Customer). The supported version that is affected is 11.4. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Relate CRM Software. While the vulnerability is in MICROS Relate CRM Software, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Relate CRM Software accessible data as well as unauthorized access to critical data or complete access to all MICROS Relate CRM Software accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2019-04-23	4.9	CVE-2018-3314 MISC
oracle -- micros_retail-j	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). The supported version that is affected is 12.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2018-2880 MISC

oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.3	CVE-2018-3123 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2566 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2580 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2581 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2584 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2585 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2587 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2589 MISC CONFIRM
oracle – mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2592 MISC CONFIRM

oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2593 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2596 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2606 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2607 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2620 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2624 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2625 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2626 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2627 MISC CONFIRM

oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2628 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2631 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2632 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2635 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2644 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2681 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2683 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2685 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2686 MISC CONFIRM

oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2687 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2688 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2689 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2691 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2693 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2694 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2695 MISC CONFIRM
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2603 MISC

oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2653 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2654 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2674 MISC
oracle -- oracle_retail_customer_engagement	Vulnerability in the Oracle Retail Customer Engagement component of Oracle Retail Applications (subcomponent: Segment). Supported versions that are affected are 16.0 and 17.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Retail Customer Engagement. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Retail Customer Engagement accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Engagement accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Engagement. CVSS 3.0 Base Score 5.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:L).	2019-04-23	6.0	CVE-2018-3312 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2609 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2610 MISC

oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2611 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2612 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2613 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).	2019-04-23	6.4	CVE-2019-2705 MISC
oracle -- peoplesoft_enterprise_elm_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM component of Oracle PeopleSoft Products (subcomponent: Enterprise Learning Mgmt). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2019-04-23	4.0	CVE-2019-2700 MISC
oracle -- peoplesoft_enterprise_human_capital_management_candidate_gateway	Vulnerability in the PeopleSoft Enterprise HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2591 MISC

oracle -- peoplesoft_enterprise_human_capital_management_talent_acquisition_manager	Vulnerability in the PeopleSoft Enterprise HCM Talent Acquisition Manager component of Oracle PeopleSoft Products (subcomponent: Job Opening). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Talent Acquisition Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Talent Acquisition Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2590 MISC
oracle -- peoplesoft_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management component of Oracle PeopleSoft Products (subcomponent: Application Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2707 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Homepage & Navigation). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2573 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: RemoteCall). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2586 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	4.9	CVE-2019-2594 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2597 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2019-04-23	5.5	CVE-2019-2598 MISC

oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2637 MISC
oracle -- primavera_p6_enterprise_project_portfolio_management	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2701 MISC
oracle -- service_bus	Vulnerability in the Oracle Service Bus component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Service Bus. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	5.0	CVE-2019-2576 MISC
oracle -- service_contracts	Vulnerability in the Oracle Service Contracts component of Oracle E-Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Service Contracts, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Service Contracts accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2622 MISC
oracle -- siebel_crm	Vulnerability in the Siebel Core - Server BizLogic Script component of Oracle Siebel CRM (subcomponent: Integration - Scripting). The supported version that is affected is 19.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server BizLogic Script accessible data as well as unauthorized read access to a subset of Siebel Core - Server BizLogic Script accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel Core - Server BizLogic Script. CVSS 3.0 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	CVE-2019-2570 MISC
oracle -- soa_suite	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Fabric Layer). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	CVE-2019-2572 MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: IPS Package Manager). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	CVE-2019-2704 MISC
oracle -- territory_management	Vulnerability in the Oracle Territory Management component of Oracle E-Business Suite (subcomponent: Territory Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Territory Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Territory Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Territory Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Territory Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2662 MISC

oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2640 MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2641 MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2642 MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2643 MISC
oracle -- transportation_management	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.3.7, 6.4.2 and 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	CVE-2019-2709 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2656 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2657 MISC

oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2680 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.4	CVE-2019-2690 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2696 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2703 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2721 MISC EXPLOIT-DB
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2722 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	CVE-2019-2723 MISC
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2578 MISC
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2579 MISC

oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N).	2019-04-23	4.0	CVE-2019-2568 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.0	CVE-2019-2615 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).	2019-04-23	5.5	CVE-2019-2618 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2647 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2648 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2649 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2650 MISC
oracle -- work_in_process	Vulnerability in the Oracle Work in Process component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	CVE-2019-2633 MISC
osticket -- osticket	In osTicket before 1.12, XSS exists via /upload/file.php, /upload/scp/users.php?do=import-users, and /upload/scp/ajax.php/users/import if an agent manager user uploads a crafted .csv file to the User Importer, because file contents can appear in an error message. The XSS can lead to local file inclusion.	2019-04-25	4.3	CVE-2019-11537 MISC MISC MISC MISC
projectsend -- projectsend	An issue was discovered in ProjectSend r1053. upload-process-form.php allows finished_files[]=../ directory traversal. It is possible for users to read arbitrary files and (potentially) access the supporting database, delete arbitrary files, access user passwords, or run arbitrary code.	2019-04-20	6.5	CVE-2019-11378 BID MISC

projectsend -- projectsend	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	4.3	CVE-2019-11533 BID CONFIRM
qemu -- qemu	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver.	2019-04-19	5.0	CVE-2019-5008 BID MISC MISC
redhat -- keycloak	Keycloak up to version 6.0.0 allows the end user token (access or id token JWT) to be used as the session cookie for browser sessions for OIDC. As a result an attacker with access to service provider backend could hijack user?s browser session.	2019-04-24	5.5	CVE-2019-3868 BID CONFIRM
redhat -- virtualization	A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product?s official releases are unaffected.	2019-04-22	4.3	CVE-2019-11463 MISC MISC
sass-lang -- libsass	The parsing component in LibSass through 3.5.5 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Parser::parse_css_variable_value in parser.cpp).	2019-04-23	4.3	CVE-2018-20821 MISC
sass-lang -- libsass	LibSass 3.5.4 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Complex_Selector::perform in ast.hpp and Sass::Inspect::operator in inspect.cpp).	2019-04-23	4.3	CVE-2018-20822 MISC
sem-cms -- semcms	An issue was discovered in SEMCMS 3.8. SEMCMS_Inquiry.php allows AID[] SQL Injection because the class.phpmailer.php inject_check_sql protection mechanism is incomplete.	2019-04-25	6.5	CVE-2019-11518 MISC
siteserver -- siteserver_cms	A issue was discovered in SiteServer CMS 6.9.0. It allows remote attackers to execute arbitrary code because an administrator can add the permitted file extension .aassp, which is converted to .asp because the “as” substring is deleted.	2019-04-22	6.5	CVE-2019-11401 MISC
struktur -- libheif	libheif 1.4.0 has a use-after-free in heif::HeifContext::Image::set_alpha_channel in heif_context.h because heif_context.cc mishandles references to non-existing alpha images.	2019-04-23	6.8	CVE-2019-11471 MISC MISC
veronalabs -- wp_statistics	The WP Statistics plugin through 12.6.2 for WordPress has XSS, allowing a remote attacker to inject arbitrary web script or HTML via the Referer header of a GET request.	2019-04-23	4.3	CVE-2019-10864 CONFIRM
verypdf -- verypdf	VeryPDF 4.1 has a Memory Overflow leading to Code Execution because pdfocx!CxImageTIF::operator in pdfocx.ocx (used by pdfeditor.exe and pdfcmd.exe) is mishandled.	2019-04-26	6.8	CVE-2019-11493 MISC
vestacp -- control_panel	Vesta Control Panel 0.9.8-23 allows XSS via a crafted URL.	2019-04-19	4.3	CVE-2019-9841 MISC CONFIRM CONFIRM
wavpack -- wavpack	WavpackSetConfiguration64 in pack_utils.c in libwavpack.a in WavPack through 5.1.0 has a “Conditional jump or move depends on uninitialised value” condition, which might allow attackers to cause a denial of service (application crash) via a DFF file that lacks valid sample-rate data.	2019-04-24	4.3	CVE-2019-11498 MISC MISC
wcms -- wcms	wcms/wex/finder/action.php in WCMS v0.3.2 has a Arbitrary File Upload Vulnerability via developer/finder because .php is a valid extension according to the fm_get_text_exts function.	2019-04-20	6.5	CVE-2019-11377 MISC MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?inform/add.html qid SQL injection.	2019-04-22	6.5	CVE-2019-11451 MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?admin_category/remove.html cid[] SQL injection.	2019-04-22	6.5	CVE-2019-11452 MISC
wifi_ftp_server_project -- wifi_ftp_server	An issue was discovered in the Medha WiFi FTP Server application 1.8.3 for Android. An attacker can read the username/password of a valid user via /data/data/com.medhaapps.wififtpserver/shared_prefs/com.medhaapps.wififtpserver_preferences.xml	2019-04-22	5.0	CVE-2019-11383 MISC
wordfence -- wordfence	The Wordfence plugin 7.2.3 for WordPress allows XSS via a unique attack vector.	2019-04-25	4.3	CVE-2019-9669 MISC
zalora -- zalora	The Zalora application 6.15.1 for Android stores confidential information insecurely on the system (i.e. plain text), which allows a non-root user to find out the username/password of a valid user via /data/data/com.zalora.android/shared_prefs/login_data.xml.	2019-04-22	5.0	CVE-2019-11384 MISC
zohocorp -- servicedesk_plus	Zoho ManageEngine ServiceDesk 9.3 allows session hijacking and privilege escalation because an established guest session is automatically converted into an established administrator session when the guest user enters the administrator username, with an arbitrary incorrect password, in an mc/ login attempt within a different browser tab.	2019-04-24	6.5	CVE-2019-10008 EXPLOIT-DB CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
audiocodes -- 405hd_firmware	A missing password verification in the web interface in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an remote attacker (in the same network as the device) to change the admin password without authentication via a POST request.	2019-04-25	3.3	CVE-2018-16219 MISC
cmsmadesimple -- cms_made_simple	The File Manager in CMS Made Simple through 2.2.10 has Reflected XSS via the “New name” field in a Rename action.	2019-04-24	3.5	CVE-2019-11513 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155999.	2019-04-25	3.5	CVE-2019-4033 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159464.	2019-04-25	3.5	CVE-2019-4238 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157107.	2019-04-25	3.5	CVE-2019-4073 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157108.	2019-04-25	3.5	CVE-2019-4074 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157109.	2019-04-25	3.5	CVE-2019-4075 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157110.	2019-04-25	3.5	CVE-2019-4076 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157111.	2019-04-25	3.5	CVE-2019-4077 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to obtain sensitive document information under unusual circumstances. IBM X-Force ID: 158401.	2019-04-25	3.5	CVE-2019-4146 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158414.	2019-04-25	3.5	CVE-2019-4148 XF CONFIRM
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Web Catalog). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N).	2019-04-23	2.6	CVE-2019-2605 MISC
oracle -- data_integrator	Vulnerability in the Oracle Data Integrator component of Oracle Fusion Middleware (subcomponent: ODI Tools). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Data Integrator accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	3.5	CVE-2019-2720 MISC

oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	3.5	CVE-2019-2614 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	3.5	CVE-2019-2617 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	3.5	CVE-2019-2623 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	3.5	CVE-2019-2630 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	1.9	CVE-2019-2634 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Procotol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	3.5	CVE-2019-2636 MISC CONFIRM
oracle -- mysql_connector/j	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2019-04-23	3.5	CVE-2019-2692 MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: File Locking Services). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	2.1	CVE-2019-2577 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	CVE-2019-2574 MISC

oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	CVE-2019-2678 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H).	2019-04-23	3.6	CVE-2019-2679 MISC
profiles_project -- profiles	XSS exists in the ProFiles 1.5 component for Joomla! via the name or path parameter when creating a new folder in the administrative panel.	2019-04-26	3.5	CVE-2018-18276 MISC
wolfcms -- wolfcms	WolfCMS 0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	CVE-2018-18823 MISC MISC MISC MISC
wolfcms -- wolfcms	WolfCMS v0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	CVE-2018-18824 MISC MISC MISC MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aikcms -- aikcms	An issue was discovered in AikCms v2.0. There is a File upload vulnerability, as demonstrated by an admin/page/system/nav.php request with PHP code in a .php file with the application/octet-stream content type.	2019-04-27	not yet calculated	CVE-2019-11568 MISC
aikcms -- aikcms	An issue was discovered in AikCms v2.0. There is a SQL Injection vulnerability via $_GET['del'], as demonstrated by an admin/page/system/nav.php?del= URI.	2019-04-27	not yet calculated	CVE-2019-11567 MISC
apache -- pluto	The input fields of the Apache Pluto “Chat Room” demo portlet 3.0.0 and 3.0.1 are vulnerable to Cross-Site Scripting (XSS) attacks. Mitigation: * Uninstall the ChatRoomDemo war file - or - * migrate to version 3.1.0 of the chat-room-demo war file	2019-04-26	not yet calculated	CVE-2019-0186 MLIST MISC BID MLIST MISC EXPLOIT-DB MLIST
apache -- qpid_proton	While investigating bug PROTON-2014, we discovered that under some circumstances Apache Qpid Proton versions 0.9 to 0.27.0 (C library and its language bindings) can connect to a peer anonymously using TLS *even when configured to verify the peer certificate* while used with OpenSSL versions before 1.1.0. This means that an undetected man in the middle attack could be constructed if an attacker can arrange to intercept TLS traffic.	2019-04-23	not yet calculated	CVE-2019-0223 MLIST BID REDHAT MISC MLIST MLIST MLIST MLIST MLIST
apache -- zeppelin	In Apache Zeppelin prior to 0.8.0 the cron scheduler was enabled by default and could allow users to run paragraphs as other users without authentication.	2019-04-23	not yet calculated	CVE-2018-1317 MLIST BID MLIST MISC
apache -- zeppelin	Apache Zeppelin prior to 0.7.3 was vulnerable to session fixation which allowed an attacker to hijack a valid user session. Issue was reported by “stone lone”.	2019-04-23	not yet calculated	CVE-2017-12619 MLIST BID MLIST MISC

apparmor -- apparmor	In all versions of AppArmor mount rules are accidentally widened when compiled.	2019-04-22	not yet calculated	CVE-2016-1585 MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 writes POST and GET parameters (including passwords) to a log file because of incorrect if/else usage in the Log-File writer component.	2019-04-24	not yet calculated	CVE-2019-9734 MISC MISC
arrow-kt -- arrow	arrow-kt Arrow before 0.9.0 resolved Gradle build artifacts (for compiling and building the published JARs) over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by an MITM attack.	2019-04-22	not yet calculated	CVE-2019-11404 MISC MISC MISC MISC MISC
asus -- zenfone_3_max_android_device	The ASUS ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_1:7.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by ASUS or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage (i.e., sdcard). The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	CVE-2018-14980 MISC MISC
asus -- zenfone_v_live_android_device	The ASUS Zenfone V Live Android device with a build fingerprint of asus/VZW_ASUS_A009/ASUS_A009:7.1.1/NMF26F/14.0610.1802.78-20180313:user/release-keys and the Asus ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_1:7.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys both contain a pre-installed platform app with a package name of com.asus.splendidcommandagent (versionCode=1510200090, versionName=1.2.0.18_160928) that contains an exported service named com.asus.splendidcommandagent.SplendidCommandAgentService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	CVE-2018-14993 MISC MISC MISC
audiocodes -- audiocodes_405hd	A command injection (missing input validation, escaping) in the monitoring or memory status web interface in AudioCodes 405HD (firmware 2.2.12) VoIP phone allows an authenticated remote attacker in the same network as the device to trigger OS commands (like starting telnetd or opening a reverse shell) via a POST request to the web server. In combination with another attack (unauthenticated password change), the attacker can circumvent the authentication requirement.	2019-04-25	not yet calculated	CVE-2018-16216 MISC
c3p0 -- c3p0	c3p0 version < 0.9.5.4 may be exploited by a billion laughs attack when loading XML configuration due to missing protections against recursive entity expansion when loading configuration.	2019-04-22	not yet calculated	CVE-2019-5427 MISC
canonical -- appoprt	Any Python module in sys.path can be imported if the command line of the process triggering the coredump is Python and the first argument is -m in Appoprt before 2.19.2 function _python_module_path.	2019-04-22	not yet calculated	CVE-2015-1341 MISC MISC
canonical -- oxide	A malicious webview could install long-lived unload handlers that reuse an incognito BrowserContext that is queued for destruction in versions of Oxide before 1.18.3.	2019-04-22	not yet calculated	CVE-2016-1586 MISC
canonical -- snapd	A vulnerability in the seccomp filters of Canonical snapd before version 2.37.4 allows a strict mode snap to insert characters into a terminal on a 64-bit host. The seccomp rules were generated to match 64-bit ioctl(2) commands on a 64-bit platform; however, the Linux kernel only uses the lower 32 bits to determine which ioctl(2) commands to run. This issue affects: Canonical snapd versions prior to 2.37.4.	2019-04-23	not yet calculated	CVE-2019-7303 MISC MISC
canonical -- snapd	snap-confine as included in snapd before 2.39 did not guard against symlink races when performing the chdir() to the current working directory of the calling user, aka a "cwd restore permission bypass."	2019-04-24	not yet calculated	CVE-2019-11503 MLIST MISC MISC
canonical -- snapd	snap-confine in snapd before 2.38 incorrectly set the ownership of a snap application to the uid and gid of the first calling user. Consequently, that user had unintended access to a private /tmp directory.	2019-04-24	not yet calculated	CVE-2019-11502 MLIST MISC MISC

canonical -- snapd	Canonical snapd before version 2.37.1 incorrectly performed socket owner validation, allowing an attacker to run arbitrary commands as root. This issue affects: Canonical snapd versions prior to 2.37.1.	2019-04-23	not yet calculated	CVE-2019-7304 MISC MISC MISC
canonical -- ubuntu_maas	A vulnerability in maasserver.api.get_file_by_name of Ubuntu MAAS allows unauthenticated network clients to download any file. This issue affects: Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	CVE-2014-1426 MISC
canonical -- ubuntu_maas	A vulnerability in generate_filestorage_key of Ubuntu MAAS allows an attacker to brute-force filenames. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	CVE-2014-1428 MISC
canonical -- ubuntu_maas	A vulnerability in the REST API of Ubuntu MAAS allows an attacker to cause a logged-in user to execute commands via cross-site scripting. This issue affects MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	CVE-2014-1427 MISC
canonical -- ubuntu_maas	The SeaMicro provisioning of Ubuntu MAAS logs credentials, including username and password, for the management interface. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	CVE-2015-1320 MISC
canonical -- ubuntu_selinux_initscript	The Ubuntu SELinux initscript before version 1:0.10 used touch to create a lockfile in a world-writable directory. If the OS kernel does not have symlink protections then an attacker can cause a zero byte file to be allocated on any writable filesystem.	2019-04-22	not yet calculated	CVE-2011-3151 MISC
cerner -- connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The hostname, timezone, and NTP server configurations on the CCE device are vulnerable to command injection by sending a crafted configuration file over the network.	2019-04-25	not yet calculated	CVE-2018-20053 MISC
cerner_connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The user running the main CCE firmware has NOPASSWD sudo privileges to several utilities that could be used to escalate privileges to root. One example is the “sudo ln -s /tmp/script /etc/cron.hourly/script” command.	2019-04-25	not yet calculated	CVE-2018-20052 MISC
check_point -- zonealarm_and_endpoint_security_client_for_windows	A hard-link created from log file archive of Check Point ZoneAlarm up to 15.4.062 or Check Point Endpoint Security client for Windows before E80.96 to any file on the system will get its permission changed so that all users can access that linked file. Doing this on files with limited access gains the local attacker higher privileges to the file.	2019-04-22	not yet calculated	CVE-2019-8452 MISC
cloud_foundry -- bosh_backup_and_restore_cli	Cloud Foundry BOSH Backup and Restore CLI, all versions prior to 1.5.0, does not check the authenticity of backup scripts in BOSH. A remote authenticated malicious user can modify the metadata file of a Bosh Backup and Restore job to request extra backup files from different jobs upon restore. The exploited hooks in this metadata script were only maintained in the cfcr-etcd-release, so clusters deployed with the BBR job for etcd in this release are vulnerable.	2019-04-24	not yet calculated	CVE-2019-3786 CONFIRM
cloud_foundry -- cf-deployment	Cloud Foundry cf-deployment, versions prior to 7.9.0, contain java components that are using an insecure protocol to fetch dependencies when building. A remote unauthenticated malicious attacker could hijack the DNS entry for the dependency, and inject malicious code into the component.	2019-04-25	not yet calculated	CVE-2019-3801 CONFIRM
cloud_foundry -- routing_release	Cloud Foundry Routing Release, all versions prior to 0.188.0, contains a vulnerability that can hijack the traffic to route services hosted outside the platform. A user with space developer permissions can create a private domain that shadows the external domain of the route service, and map that route to an app. When the gorouter receives traffic destined for the external route service, this traffic will instead be directed to the internal app using the shadow route.	2019-04-24	not yet calculated	CVE-2019-3789 CONFIRM
cloud_foundry -- uaa_release	Cloud Foundry UAA Release, versions prior to 71.0, allows clients to be configured with an insecure redirect uri. Given a UAA client was configured with a wildcard in the redirect uri’s subdomain, a remote malicious unauthenticated user can craft a phishing link to get a UAA access code from the victim.	2019-04-25	not yet calculated	CVE-2019-3788 CONFIRM
contao -- contao	Contao 3.0.0 to 3.5.30 and 4.0.0 to 4.4.7 contains an SQL injection vulnerability in the back end as well as in the listing module.	2019-04-25	not yet calculated	CVE-2017-16558 CONFIRM CONFIRM
cribl -- cribl_ui	Cribl UI 1.5.0 allows remote attackers to run arbitrary commands via an unauthenticated web request.	2019-04-23	not yet calculated	CVE-2019-11076 CONFIRM MISC
daviewindy -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed Image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	not yet calculated	CVE-2019-9137 MISC
dell_emc -- idrac	Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.	2019-04-26	not yet calculated	CVE-2019-3705 MISC

dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.30.30.30 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted input data to the WS-MAN interface.	2019-04-22	not yet calculated	CVE-2019-3707 MISC
dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.24.24.24, 3.21.26.22, 3.22.22.22 and 3.21.25.22 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted data to the iDRAC web interface.	2019-04-22	not yet calculated	CVE-2019-3706 MISC
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain a Directory Traversal Vulnerability. A remote authenticated malicious user with admin privileges could potentially exploit this vulnerability to gain unauthorized access to the file system by exploiting insufficient sanitization of input parameters.	2019-04-25	not yet calculated	CVE-2019-3720 MISC
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain an Improper Range Header Processing Vulnerability. A remote unauthenticated attacker may send crafted requests with overlapping ranges to cause the application to compress each of the requested bytes, resulting in a crash due to excessive memory consumption and preventing users from accessing the system.	2019-04-25	not yet calculated	CVE-2019-3721 MISC
deltek -- vision	Deltek Vision 7.x before 7.6 permits the execution of any attacker supplied SQL statement through a custom RPC over HTTP protocol. The Vision system relies on the client binary to enforce security rules and integrity of SQL statements and other content being sent to the server. Client HTTP calls can be manipulated by one of several means to execute arbitrary SQL statements (similar to SQLi) or possibly have unspecified other impact via this custom protocol. To perform these attacks an authenticated session is first required. In some cases client calls are obfuscated by encryption, which can be bypassed due to hard-coded keys and an insecure key rotation protocol. Impacts may include remote code execution in some deployments; however, the vendor states that this cannot occur when the installation documentation is heeded.	2019-04-24	not yet calculated	CVE-2018-18251 CONFIRM
dentsply_sirona -- sidexis	A default username and password in Dentsply Sirona Sidexis 4.2 and possibly others allows an attacker to gain administrative access to the application server.	2019-04-24	not yet calculated	CVE-2019-11081 MISC
dillon_kane_group -- tidal_workload_automation_agent	An issue was discovered in Dillon Kane Tidal Workload Automation Agent 3.2.0.5 (formerly known as Cisco Workload Automation or CWA). The Enterprise Scheduler for AIX allows local users to gain privileges via Command Injection in crafted Tidal Job Buffers (TJB) parameters. NOTE: this vulnerability exists because the CVE-2014-3272 solution did not address AIX operating systems.	2019-04-26	not yet calculated	CVE-2019-6689 MISC
dovecot -- dovecot	The JSON encoder in Dovecot before 2.3.5.2 allows attackers to repeatedly crash the authentication service by attempting to authenticate with an invalid UTF-8 sequence as the username.	2019-04-24	not yet calculated	CVE-2019-10691 MLIST MLIST
dropbox -- lepton	io/ZlibCompression.cc in the decompression component in Dropbox Lepton 1.2.1 allows attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact by crafting a jpg image file. The root cause is a missing check of header payloads that may be (incorrectly) larger than the maximum file size.	2019-04-23	not yet calculated	CVE-2018-20819 MISC
eclipse -- jetty	In Eclipse Jetty version 7.x, 8.x, 9.2.27 and older, 9.3.26 and older, and 9.4.16 and older, the server running on any OS and Jetty version combination will reveal the configured fully qualified directory base resource location on the output of the 404 error for not finding a Context that matches the requested path. The default server behavior on jetty-distribution and jetty-home will include at the end of the Handler tree a DefaultHandler, which is responsible for reporting this 404 error, it presents the various configured contexts as HTML for users to click through to. This produced HTML includes output that contains the configured fully qualified directory base resource location for each context.	2019-04-22	not yet calculated	CVE-2019-10247 CONFIRM
eclipse -- jetty	In Eclipse Jetty version 9.2.27, 9.3.26, and 9.4.16, the server running on Windows is vulnerable to exposure of the fully qualified Base Resource directory name on Windows to a remote client when it is configured for showing a Listing of directory contents. This information reveal is restricted to only the content in the configured base resource directories.	2019-04-22	not yet calculated	CVE-2019-10246 CONFIRM
eclipse -- openj9	In Eclipse OpenJ9 prior to the 0.14.0 release, the Java bytecode verifier incorrectly allows a method to execute past the end of bytecode array causing crashes. Eclipse OpenJ9 v0.14.0 correctly detects this case and rejects the attempted class load.	2019-04-19	not yet calculated	CVE-2019-10245 CONFIRM
eclipse -- vorto	Eclipse Vorto versions prior to 0.11 resolved Maven build artifacts for the Xtext project over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by a MITM attack. Hence produced build artifacts of Vorto might be infected.	2019-04-22	not yet calculated	CVE-2019-10248 CONFIRM
ekiga -- ekiga	Ekiga versions before 3.3.0 attempted to load a module from /tmp/ekiga_test.so.	2019-04-22	not yet calculated	CVE-2011-1830 MISC

envoy_proxy -- envoy	When parsing HTTP/1.x header values, Envoy 1.9.0 and before does not reject embedded zero characters (NUL, ASCII 0x0). This allows remote attackers crafting header values containing embedded NUL characters to potentially bypass header matching rules, gaining access to unauthorized resources.	2019-04-25	not yet calculated	CVE-2019-9900 REDHAT CONFIRM CONFIRM CONFIRM
envoy_proxy -- envoy	Envoy 1.9.0 and before does not normalize HTTP URL paths. A remote attacker may craft a relative path, e.g., something/../admin, to bypass access control, e.g., a block on /admin. A backend server could then interpret the non-normalized path and provide an attacker access beyond the scope provided for by the access control policy.	2019-04-25	not yet calculated	CVE-2019-9901 CONFIRM CONFIRM CONFIRM
essential_products -- phone_android_device	The Essential Phone Android device with a build fingerprint of essential/mata/mata:8.1.0/OPM1.180104.166/297:user/release-keys contains a pre-installed platform app with a package name of com.ts.android.hiddenmenu (versionName=1.0, platformBuildVersionName=8.1.0) that contains an exported activity app component named com.ts.android.hiddenmenu.rtn.RTNResetActivity that allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-14994 MISC MISC MISC
flarum -- flarum	User/Command/ConfirmEmailHandler.php in Flarum before 0.1.0-beta.8 mishandles invalidation of user email tokens.	2019-04-24	not yet calculated	CVE-2019-11514 MISC MISC
gitea -- gitea	Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.	2019-04-27	not yet calculated	CVE-2019-11576 MISC MISC
gnome -- nautilus	An issue was discovered in GNOME Nautilus 3.30 prior to 3.30.6 and 3.32 prior to 3.32.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	not yet calculated	CVE-2019-11461 MISC
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/faqmasterformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15581 CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/boardgroup_form_update.php and adm/boardgroup_list_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15584 CONFIRM CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/sms_admin/num_book_write.php and adm/sms_admin/num_book_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15582 CONFIRM CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/contentformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15580 CONFIRM
google -- tensorflow	Invalid memory access and/or a heap buffer overflow in the TensorFlow XLA compiler in Google TensorFlow before 1.7.1 could cause a crash or read from other parts of process memory via a crafted configuration file.	2019-04-24	not yet calculated	CVE-2018-10055 CONFIRM
google -- tensorflow	Google TensorFlow 1.7.x and earlier is affected by a Buffer Overflow vulnerability. The type of exploitation is context-dependent.	2019-04-24	not yet calculated	CVE-2018-7575 CONFIRM
google -- tensorflow	Memcpy parameter overlap in Google Snappy library 1.1.4, as used in Google TensorFlow before 1.7.1, could result in a crash or read from other parts of process memory.	2019-04-24	not yet calculated	CVE-2018-7577 CONFIRM
google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by a Null Pointer Dereference vulnerability. The type of exploitation is: context-dependent.	2019-04-24	not yet calculated	CVE-2018-7574 CONFIRM
heketi -- heketi	It was found that default configuration of Heketi does not require any authentication potentially exposing the management interface to misuse. This isue only affects heketi as shipped with Openshift Container Platform 3.11.	2019-04-22	not yet calculated	CVE-2019-3899 CONFIRM
hisilicon -- hi3510_firmware	Incorrect access control in the RTSP stream and web portal on all IP cameras based on Hisilicon Hi3510 firmware (until Webware version V1.0.1) allows attackers to view an RTSP stream by connecting to the stream with hidden credentials (guest or user) that are neither displayed nor configurable in the camera's CamHi or keye mobile management application. This affects certain devices labeled as HI3510, HI3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Unitoptek, ESCAM, etc.	2019-04-23	not yet calculated	CVE-2019-10711 MISC

hisilicon -- hi3510_firmware	Insecure permissions in the Web management portal on all IP cameras based on Hisilicon Hi3510 firmware allow authenticated attackers to receive a network's cleartext WiFi credentials via a specific HTTP request. This affects certain devices labeled as HI3510, HI3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Unitoptek, ESCAM, etc.	2019-04-23	not yet calculated	CVE-2019-10710 MISC
hostapd_and_wpa_supplicant -- hostapd_and_wpa_supplicant	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	2019-04-26	not yet calculated	CVE-2019-11555 MLIST MISC MISC MISC
hr-technologies -- easytorecruit	In EasyToRecruit (E2R) before 2.11, the upload feature and the Candidate Profile Management feature are prone to Cross Site Scripting (XSS) injection in multiple locations.	2019-04-24	not yet calculated	CVE-2019-11032 MISC MISC
ibm -- mq	IBM MQ 8.0.0.0 through 8.0.0.10, 9.0.0.0 through 9.0.0.5, and 9.1.0.0 through 9.1.1 is vulnerable to a denial of service attack within the TLS key renegotiation function. IBM X-Force ID: 156564.	2019-04-19	not yet calculated	CVE-2019-4055 BID XF CONFIRM
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.1, 5.2.6.3_6, 6.0.0.0, and 6.0.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 147294.	2019-04-25	not yet calculated	CVE-2018-1720 XF CONFIRM
imperva -- securesphere	A command injection vulnerability in PWS in Imperva SecureSphere 13.0.0.10 and 13.1.0.10 Gateway allows an attacker with authenticated access to execute arbitrary OS commands on a vulnerable installation.	2019-04-25	not yet calculated	CVE-2018-16660 MISC MISC
jakub_chodounsky -- bonobo_git_server	Improper handling of extra parameters in the AccountController (User Profile edit) in Jakub Chodounsky Bonobo Git Server before 6.5.0 allows authenticated users to gain application administrator privileges via additional form parameter submissions.	2019-04-24	not yet calculated	CVE-2019-11218 CONFIRM MISC
jakub_chodounsky -- bonobo_git_server	The GitController in Jakub Chodounsky Bonobo Git Server before 6.5.0 allows execution of arbitrary commands in the context of the web server via a crafted http request.	2019-04-24	not yet calculated	CVE-2019-11217 CONFIRM MISC
juju_core -- joyent_provider	Juju Core's Joyent provider before version 1.25.5 uploads the user's private ssh key.	2019-04-22	not yet calculated	CVE-2015-1316 MISC
kubernetes -- kubernetes	In Kubernetes v1.8.x-v1.14.x, schema info is cached by kubectl in the location specified by --cache-dir (defaulting to $HOME/.kube/http-cache), written with world-writeable permissions (rw-rw-rw-). If --cache-dir is specified and pointed at a different location accessible to other users/groups, the written files may be modified by other users/groups and disrupt the kubectl invocation.	2019-04-22	not yet calculated	CVE-2019-11244 BID MISC
leagoo -- p1_android_device	The Leagoo P1 Android device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains the android framework (i.e., system_server) with a package name of android that has been modified by Leagoo or another entity in the supply chain. The system_server process in the core Android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	CVE-2018-14997 MISC MISC MISC
leagoo -- p1_android_device	The Leagoo P1 device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains a pre-installed platform app with a package name of com.wtk.factory (versionCode=1, versionName=1.0) that contains an exported broadcast receiver named com.wtk.factory.MMITestReceiver allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-14999 MISC MISC MISC
lenovo -- system_x	In various firmware versions of Lenovo System x, the integrated management module II (IMM2)'s first failure data capture (FFDC) includes the web server's private key in the generated log file for support.	2019-04-22	not yet calculated	CVE-2019-6157 MISC

librenms -- librenms	LibreNMS 1.46 allows remote attackers to execute arbitrary OS commands by using the $_POST['community'] parameter to html/pages/addhost.inc.php during creation of a new device, and then making a /ajax_output.php?id=capture&format=text&type=snmpwalk&hostname=localhost request that triggers html/includes/output/capture.inc.php command mishandling.	2019-04-24	not yet calculated	CVE-2018-20434 MISC MISC MISC
libseccomp-golang -- libseccomp-golang	libseccomp-golang 0.9.0 and earlier incorrectly generates BPFs that OR multiple arguments rather than ANDing them. A process running under a restrictive seccomp filter that specified multiple syscall arguments could bypass intended access restrictions by specifying a single matching argument.	2019-04-24	not yet calculated	CVE-2017-18367 MLIST MISC MISC
liferay -- portal_community_edition	An issue was discovered in Liferay Portal CE 7.1.2 GA3. An attacker can use Liferay's Groovy script console to execute OS commands. Commands can be executed via a [command].execute() call, as demonstrated by "def cmd =" in the ServerAdminPortlet_script value to group/control_panel/manage. Valid credentials for an application administrator user account are required.	2019-04-22	not yet calculated	CVE-2019-11444 MISC MISC
linux -- linux_kernel	The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.	2019-04-23	not yet calculated	CVE-2019-11487 BID MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
linux -- linux_kernel	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.	2019-04-25	not yet calculated	CVE-2019-3900 BID CONFIRM CONFIRM
linux -- linux_kernel	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.	2019-04-24	not yet calculated	CVE-2019-3882 CONFIRM
linux -- linux_kernel	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As no relevant locks (in particular the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target task to perform an execve() syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass the ptrace_may_access() check and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve() calls. This issue affects kernel versions before 4.8.	2019-04-22	not yet calculated	CVE-2019-3901 BID CONFIRM
lxd -- lxd	LXD before version 0.19-0ubuntu5 doUidshiftIntoContainer() has an unsafe Chmod() call that races against the stat in the Filepath.Walk() function. A symbolic link created in that window could cause any file on the system to have any mode of the attacker's choice.	2019-04-22	not yet calculated	CVE-2015-1340 MISC
mercurial -- mercurial	A flaw was found in Mercurial before 4.9. It was possible to use symlinks and subrepositories to defeat Mercurial's path-checking logic and write files outside a repository.	2019-04-22	not yet calculated	CVE-2019-3902 CONFIRM MLIST MISC
mount.ecrpytfs_private -- mount.ecrpytfs_private	When mount.ecrpytfs_private before version 87-0ubuntu1.2 calls setreuid() it doesn't also set the effective group id. So when it creates the new version, mtab.tmp, it's created with the group id of the user running mount.ecryptfs_private.	2019-04-22	not yet calculated	CVE-2011-3145 MISC
mozilla -- firefox	On Android systems, Firefox can load a library from APITRACE_LIB, which is writable by all users and applications. This could allow malicious third party applications to execute a man-in-the-middle attack if a malicious code was written to that location and loaded. *Note: This issue only affects Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9798 MISC MISC
mozilla -- firefox	A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9805 MISC MISC
mozilla -- firefox	In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. *Note: This issue only affects macOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9804 MISC MISC

mozilla -- firefox	Insufficient bounds checking of data during inter-process communication might allow a compromised content process to be able to read memory from the parent process under certain conditions. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9799 MISC MISC
mozilla -- firefox	The Upgrade-Insecure-Requests (UIR) specification states that if UIR is enabled through Content Security Policy (CSP), navigation to a same-origin URL must be upgraded to HTTPS. Firefox will incorrectly navigate to an HTTP URL rather than perform the security upgrade requested by the CSP in some circumstances, allowing for potential man-in-the-middle attacks on the linked resources. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9803 MISC MISC MISC MISC
mozilla -- firefox	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.	2019-04-26	not yet calculated	CVE-2018-5179 MISC
mozilla -- firefox	Unsanitized output in the browser UI leaves HTML tags in place and can result in arbitrary code execution in Firefox before version 58.0.1.	2019-04-26	not yet calculated	CVE-2018-5124 MISC
mozilla -- firefox	Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9797 MISC MISC
mozilla -- firefox	A vulnerability exists during authorization prompting for FTP transaction where successive modal prompts are displayed and cannot be immediately dismissed. This allows for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9806 MISC MISC
mozilla -- firefox	If a Sandbox content process is compromised, it can initiate an FTP download which will then use a child process to render the downloaded data. The downloaded data can then be passed to the Chrome process with an arbitrary file length supplied by an attacker, bypassing sandbox protections and allow for a potential memory read of adjacent data from the privileged Chrome process, which may include sensitive data. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9802 MISC MISC
mozilla -- firefox	Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. *Note: This only affects Firefox 65. Previous versions are unaffected.*. This vulnerability affects Firefox < 65.0.1.	2019-04-26	not yet calculated	CVE-2018-18511 MISC MISC
mozilla -- firefox	When arbitrary text is sent over an FTP connection and a page reload is initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9807 MISC MISC
mozilla -- firefox	If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states “Unknown origin” as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9808 MISC MISC
mozilla -- firefox	If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9809 MISC MISC MISC
mozilla -- thunderbird	A crash can occur when processing a crafted S/MIME message or an XPI package containing a crafted signature. This can be used as a denial-of-service (DOS) attack because Thunderbird reopens the last seen message on restart, triggering the crash again. This vulnerability affects Thunderbird < 60.5.	2019-04-26	not yet calculated	CVE-2018-18513 MISC MISC
mozilla -- thunderbird	A flaw during verification of certain S/MIME signatures causes emails to be shown in Thunderbird as having a valid digital signature, even if the shown message contents aren’t covered by the signature. The flaw allows an attacker to reuse a valid S/MIME signature to craft an email message with arbitrary content. This vulnerability affects Thunderbird < 60.5.1.	2019-04-26	not yet calculated	CVE-2018-18509 MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9794 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	CVE-2019-9810 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	CVE-2019-9813 MISC MISC MISC MISC

mozilla -- thunderbird_and_firefox_esr_and_firefox	Firefox will accept any registered Program ID as an external protocol handler and offer to launch this local application when given a matching URL on Windows operating systems. This should only happen if the program has specifically registered itself as a "URL Handler" in the Windows registry. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9801 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. *Note: Spectre mitigations are currently enabled for all users by default settings.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9793 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9792 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9791 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9795 MISC MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9796 MISC MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with a broadcast receiver app component named com.suntek.mway.rcs.app.test.TestReceiver and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a broadcast receiver app component named com.rcs.gsma.na.test.TestReceiver allow any app co-located on the device to programmatically send text messages where the number and body of the text message is controlled by the attacker due to an exported broadcast receiver app component. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. A separate vulnerability in the app allows a zero-permission app to programmatically delete text messages, so the sent text messages can be removed to not alert the user.	2019-04-25	not yet calculated	CVE-2018-14990 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with an exported content provider named com.suntek.mway.rcs.app.service.provider.message.MessageProvider and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a content provider named com.rcs.gsma.na.provider.message.MessageProvider allow any app co-located on the device to read, write, insert, and modify the user's text messages. This is enabled by an exported content provider app component that serves as a wrapper to the official content provider that contains the user's text messages. This app cannot be disabled by the user and the attack can be performed by a zero-permission app.	2019-04-25	not yet calculated	CVE-2018-14991 MISC MISC MISC

multiple_vendors -- multiple_products	The Coolpad Defiant (Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys) and the T-Mobile Revvl Plus (Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys) Android devices contain a pre-installed platform app with a package name of com.qualcomm.qti.telephony.extcarrierpack (versionCode=25, versionName=7.1.1) containing an exported broadcast receiver app component named com.qualcomm.qti.telephony.extcarrierpack.UiccReceiver that allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-15003 MISC MISC MISC
nopcommerce -- nopcommerce	Libraries/Nop.Services/Localization/LocalizationService.cs in nopCommerce through 4.10 allows XXE via the "Configurations -> Languages -> Edit Language -> Import Resources -> Upload XML file" screen.	2019-04-25	not yet calculated	CVE-2019-11519 MISC MISC
omniauth_ruby_gem -- omniauth_ruby_gem	The request phase of the OmniAuth Ruby gem is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the primary account.	2019-04-26	not yet calculated	CVE-2015-9284 MISC MISC MLIST
openapi_tools -- openapi_generator	OpenAPI Tools OpenAPI Generator before 4.0.0-20190419.052012-560 uses http:// URLs in various build.gradle, build.gradle.mustache, and build.sbt files, which may have caused insecurely resolved dependencies.	2019-04-22	not yet calculated	CVE-2019-11405 MISC MISC MISC
oppo -- f5_android_device	The Oppo F5 Android device with a build fingerprint of OPPO/CPH1723/CPH1723:7.1.1/N6F26Q/1513597833:user/release-keys contains a pre-installed platform app with a package name of com.dropboxchmod (versionCode=1, versionName=1.0) that contains an exported service named com.dropboxchmod.DropboxChmodService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), and obtains the user's text messages, and more. This vulnerability can also be used to secretly record audio of the user without their awareness on the Oppo F5 device. The pre-installed com.oppo.engineermode app (versionCode=25, versionName=V1.01) has an exported activity that can be started to initiate a recording and quickly dismissed. The activity can be started in a way that the user will not be able to see the app in the recent apps list. The resulting audio amr file can be copied from a location on internal storage using the arbitrary command execution as system user vulnerability. Executing commands as system user can allow a third-party app to factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	CVE-2018-14996 MISC MISC MISC
oracle -- berkeley_db	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are Prior to 6.138, prior to 6.2.38 and prior to 18.1.32. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Data Store. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	not yet calculated	CVE-2019-2708 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-26	not yet calculated	CVE-2019-2725 MISC
phablet-team -- content_hub	Content Hub before version 0.0+15.04.20150331-0ubuntu1.0 DBUS API only requires a file path for a content item, it doesn't actually require the confined app have access to the file to create a transfer. This could allow a malicious application using the DBUS API to export file:///etc/passwd which would then send a copy of that file to another app.	2019-04-22	not yet calculated	CVE-2015-1327 MISC
phablet-team -- ubuntu-download-manager	UDM provides support for running commands after a download is completed, this is currently made use of for click package installation. This functionality was not restricted to unconfined applications. Before UDM version 1.2+16.04.20160408-0ubuntu1 any confined application could make use of the UDM C++ API to run arbitrary commands in an unconfined environment as the phablet user.	2019-04-22	not yet calculated	CVE-2016-1579 MISC

pivotal -- apps_manager_release	Pivotal Apps Manager Release, versions 665.0.x prior to 665.0.28, versions 666.0.x prior to 666.0.21, versions 667.0.x prior to 667.0.7, contain an invitation service that accepts HTTP. A remote unauthenticated user could listen to network traffic and gain access to the authorization credentials used to make the invitation requests.	2019-04-24	not yet calculated	CVE-2019-3793 CONFIRM
plum -- compass_android_device	The Plum Compass Android device with a build fingerprint of PLUM/c179_hwf_221/c179_hwf_221:6.0/MRA58K/W16.51.5-22:user/release-keys contains a pre-installed platform app with a package name of com.android.settings (versionCode=23, versionName=6.0-eng.root.20161223.224055) that contains an exported broadcast receiver app component which allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-14989 MISC MISC MISC
polycom -- vvx_products_using_ucs_software	VVX products using UCS software version 5.8.0 and earlier with Better Together over Ethernet Connector (BToE) application version 3.8.0 and earlier uses hard-coded credentials to establish a connection between the host application and device.	2019-04-23	not yet calculated	CVE-2019-10688 CONFIRM
printeron -- printeron	An XML external entity (XXE) vulnerability in PrinterOn version 4.1.4 and lower allows remote authenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.	2019-04-23	not yet calculated	CVE-2018-17169 MISC
projectsend -- projectsend	ProjectSend before r1070 writes user passwords to the server logs.	2019-04-26	not yet calculated	CVE-2019-11492 CONFIRM
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4 and 8.3RX before 8.3R7.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2 and 5.4RX before 5.4R7.1, an unauthenticated, remote attacker can conduct a session hijacking attack.	2019-04-25	not yet calculated	CVE-2019-11540 BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.2RX before 8.2R12.1, users using SAML authentication with the Reuse Existing NC (Pulse) Session option may see authentication leaks.	2019-04-25	not yet calculated	CVE-2019-11541 BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, an authenticated attacker (via the admin web interface) can send a specially crafted message resulting in a stack buffer overflow.	2019-04-25	not yet calculated	CVE-2019-11542 BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, the admin web interface allows an authenticated attacker to inject and execute commands.	2019-04-25	not yet calculated	CVE-2019-11539 BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1, an NFS problem could allow an authenticated attacker to access the contents of arbitrary files on the affected device.	2019-04-25	not yet calculated	CVE-2019-11538 BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	XSS exists in the admin web console in Pulse Secure Pulse Connect Secure (PCS) 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, and 5.2RX before 5.2R12.1.	2019-04-25	not yet calculated	CVE-2019-11543 BID CONFIRM MISC
python-dbusmock -- python-dbusmock	python-dbusmock before version 0.15.1 AddTemplate() D-Bus method call or DBusTestCase.spawn_server_template() method could be tricked into executing malicious code if an attacker supplies a .pyc file.	2019-04-22	not yet calculated	CVE-2015-1326 MISC
robotronic -- runasspc	Robotronic RunAsSpc 3.7.0.0 protects stored credentials insufficiently, which allows locally authenticated attackers (under the same user context) to obtain cleartext credentials of the stored account.	2019-04-24	not yet calculated	CVE-2019-10239 MISC
rockwell_automation -- micrologix_and_compactlogix_controllers	In Rockwell Automation MicroLogix 1400 Controllers Series A, All Versions Series B, v15.002 and earlier, MicroLogix 1100 Controllers v14.00 and earlier, CompactLogix 5370 L1 controllers v30.014 and earlier, CompactLogix 5370 L2 controllers v30.014 and earlier, CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix controllers) v30.014 and earlier, an open redirect vulnerability could allow a remote unauthenticated attacker to input a malicious link to redirect users to a malicious site that could run or download arbitrary malware on the user?s machine.	2019-04-25	not yet calculated	CVE-2019-10955 MISC BID
shenzhen_yunni_technology -- ilnkp2p	An authentication flaw in Shenzhen Yunni Technology iLnkP2P allows remote attackers to actively intercept user-to-device traffic in cleartext, including video streams and device credentials.	2019-04-26	not yet calculated	CVE-2019-11220 MISC

shenzhen_yunni_technology -- ilnkp2p	The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	2019-04-26	not yet calculated	CVE-2019-11219 MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Administrative Management Interface in SimplyBook.me Enterprise before 2019-04-23 allows Authenticated Low-Priv Users to Elevate Privileges to Full Admin Rights via a crafted HTTP PUT Request, as demonstrated by modified JSON data to a /v2/rest/ URI.	2019-04-25	not yet calculated	CVE-2019-11489 MISC MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Account Access / Password Reset Link in SimplyBook.me Enterprise before 2019-04-23 allows Unauthorized Attackers to READ/WRITE Customer or Administrator data via a persistent HTTP GET Request Hash Link Replay, as demonstrated by a login-link from the browser history.	2019-04-25	not yet calculated	CVE-2019-11488 MISC MISC
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6995 has stored XSS. JavaScript code could be executed on the application by opening a malicious email or when viewing a malicious file attachment.	2019-04-24	not yet calculated	CVE-2019-7211 MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows deserialization of untrusted data. An unauthenticated attacker could run commands on the server when port 17001 was remotely accessible. This port is not accessible remotely by default after applying the Build 6985 patch.	2019-04-24	not yet calculated	CVE-2019-7214 MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows directory traversal. An authenticated user could delete arbitrary files or could create files in new folders in arbitrary locations on the mail server. This could lead to command execution on the server for instance by putting files inside the web directories.	2019-04-24	not yet calculated	CVE-2019-7213 MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 has hardcoded secret keys. An unauthenticated attacker could access other users? emails and file attachments. It was also possible to interact with mailing lists.	2019-04-24	not yet calculated	CVE-2019-7212 MISC CONFIRM
snapcore -- snapweb	The Snapweb interface before version 0.21.2 was exposing controls to install or remove snap packages without controlling the identity of the user, nor the origin of the connection. An attacker could have used the controls to remotely add a valid, but malicious, snap package, from the Store, potentially using system resources without permission from the legitimate administrator of the system.	2019-04-22	not yet calculated	CVE-2016-1587 MISC
sonicwall -- global_management_system	A vulnerability in SonicWall Global Management System (GMS), allow a remote user to gain access to the appliance using existing SSH key. This vulnerability affects GMS versions 9.1, 9.0, 8.7, 8.6, 8.4, 8.3 and earlier.	2019-04-26	not yet calculated	CVE-2019-7476 CONFIRM
sony -- photo_sharing_plus_application	An incorrect access control exists in the Sony Photo Sharing Plus application in the firmware before PKG6.5629 version (for the X7500D TV and other applicable TVs). This vulnerability allows an attacker to read arbitrary files without authentication over HTTP when Photo Sharing Plus application is running. This may allow an attacker to browse a particular directory (e.g. images) inside the private network.	2019-04-19	not yet calculated	CVE-2019-10886 MISC FULLDISC BID BUGTRAQ CONFIRM
sony -- xperia_l1_android_device	The Sony Xperia L1 Android device with a build fingerprint of Sony/G3313/G3313:7.0/43.0.A.6.49/2867558199:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by Sony or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	CVE-2018-14983 MISC MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	CVE-2018-18367 BID CONFIRM
symantec -- endpoint_protection_manager	SEP (Mac client) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a CSV/DDE injection (also known as formula injection) vulnerability, which is a type of issue whereby an application or website allows untrusted input into CSV files.	2019-04-25	not yet calculated	CVE-2018-12244 MISC BID

symantec -- norton_security	Symantec Norton Security prior to 22.16.3, SEP (Windows client) prior to and including 12.1 RU6 MP9, and prior to 14.2 RU1, SEP SBE prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22, SEP-12.1.7484.7002 and SEP Cloud prior to 22.16.3 may be susceptible to a kernel memory disclosure, which is a type of issue where a specially crafted IRP request can cause the driver to return uninitialized memory.	2019-04-25	not yet calculated	CVE-2018-18366 BID CONFIRM
symantec -- norton_security	Norton Security (Windows client) prior to 22.16.3 and SEP SBE (Windows client) prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22 & SEP-12.1.7484.7002, may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	CVE-2018-18369 BID CONFIRM
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	2019-04-26	not yet calculated	CVE-2019-3844 CONFIRM
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	2019-04-26	not yet calculated	CVE-2019-3843 CONFIRM FEDORA
teamspeak_systems -- teamspeak_3_client	TeamSpeak 3 Client before 3.2.5 allows remote code execution in the Qt framework.	2019-04-19	not yet calculated	CVE-2019-11351 MISC MISC
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the page parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, a causing buffer overflow.	2019-04-25	not yet calculated	CVE-2018-14557 MISC
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the list parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, causing a buffer overflow.	2019-04-25	not yet calculated	CVE-2018-14559 MISC
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability wherein a user without privileges to upload distributed application archives ("Upload DAA" permission) can theoretically upload arbitrary code, and in some circumstances then execute that code on ActiveMatrix Service Grid nodes. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	CVE-2019-8992 BID MISC MISC
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client, openspace client, and app development client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain a vulnerability wherein a malicious URL could trick a user into visiting a website of the attacker's choice. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	CVE-2019-8995 BID MISC MISC
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contains vulnerabilities where an authenticated user can change settings that can theoretically adversely impact other users. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	CVE-2019-8994 BID MISC MISC

tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative web server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability that could theoretically allow an unauthenticated user to download a file with credentials information. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	CVE-2019-8993 BID MISC MISC
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrator web interface of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains multiple vulnerabilities that may allow for cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	CVE-2019-8991 BID MISC MISC
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client, openspace client, app development client, and REST API of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain cross site scripting (XSS) and cross-site request forgery vulnerabilities. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	CVE-2019-11203 BID MISC MISC
tildeslash -- m/monit	An issue was discovered in /admin/users/update in M/Monit before 3.7.3. It allows unprivileged users to escalate their privileges to an administrator by requesting a password change and specifying the admin parameter.	2019-04-22	not yet calculated	CVE-2019-11393 MISC MISC
tildeslash -- monit	A buffer over-read in Util_urlDecode in util.c in Tildeslash Monit before 5.25.3 allows a remote authenticated attacker to retrieve the contents of adjacent memory via manipulation of GET or POST parameters. The attacker can also cause a denial of service (application outage).	2019-04-22	not yet calculated	CVE-2019-11455 MISC MISC MISC MLIST
tildeslash -- monit	Persistent cross-site scripting (XSS) in http/cervlet.c in Tildeslash Monit before 5.25.3 allows a remote unauthenticated attacker to introduce arbitrary JavaScript via manipulation of an unsanitized user field of the Authorization header for HTTP Basic Authentication, which is mishandled during an _viewlog operation.	2019-04-22	not yet calculated	CVE-2019-11454 MISC MISC MISC MLIST
unity-scope-gdrive_logs -- unity-scope-gdrive_logs	All versions of unity-scope-gdrive logs search terms to syslog.	2019-04-22	not yet calculated	CVE-2015-1343 MISC
unity8-team -- unity8	Versions of Unity8 before 8.11+16.04.20160122-0ubuntu1 file plugins/Dash/CardCreator.js will execute any code found in place of a fallback image supplied by a scope.	2019-04-22	not yet calculated	CVE-2016-1573 MISC
unity8-team -- unity8	In all versions of Unity8 a running but not active application on a large-screen device could talk with Maliit and consume keyboard input.	2019-04-22	not yet calculated	CVE-2016-1584 MISC
vivo -- v7_android_device	The Vivo V7 Android device with a build fingerprint of vivo/1718/1718:7.1.2/N2G47H/compil11021857:user/release-keys contains a platform app with a package name of com.vivo.smartshot (versionCode=1, versionName=3.0.0). This app contains an exported service named com.vivo.smartshot.ui.service.ScreenRecordService that will record the screen for 60 minutes and write the mp4 file to a location of the user's choosing. Normally, a recording notification will be visible to the user, but we discovered an approach to make it mostly transparent to the user by quickly removing a notification and floating icon. The user can see a floating icon and notification appear and disappear quickly due to quickly stopping and restarting the service with different parameters that do not interfere with the ongoing screen recording. The screen recording lasts for 60 minutes and can be written directly to the attacking app's private directory.	2019-04-25	not yet calculated	CVE-2018-15000 MISC MISC MISC

western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an authentication bypass vulnerability. The login_mgr.cgi file checks credentials against /etc/shadow. However, the “nobody” account (which can be used to access the control panel API as a low-privilege logged-in user) has a default empty password, allowing an attacker to modify the My Cloud EX2 Ultra web page source code and obtain access to the My Cloud as a non-Admin My Cloud device user.	2019-04-24	not yet calculated	CVE-2019-9950 CONFIRM CONFIRM
western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an unauthenticated file upload vulnerability. The page web/jquery/uploader/uploadify.php can be accessed without any credentials, and allows uploading arbitrary files to any location on the attached storage.	2019-04-24	not yet calculated	CVE-2019-9951 CONFIRM CONFIRM
wordpress -- wordpress	Server Side Request Forgery (SSRF) exists in the Print My Blog plugin before 1.6.7 for WordPress via the site parameter.	2019-04-27	not yet calculated	CVE-2019-11565 MISC MISC MISC MISC MISC
wordpress -- wordpress	The WebDorado Contact Form Builder plugin before 1.0.69 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the $_POST[‘action’] value and the $_GET[‘action’] value, and the latter is unsanitized.	2019-04-26	not yet calculated	CVE-2019-11557 MISC MISC
xiaomi -- mi_5s_devices	The gyroscope on Xiaomi Mi 5s devices allows attackers to cause a denial of service (resonance and false data) via a 20.4 kHz audio signal, aka a MEMS ultrasound attack.	2019-04-25	not yet calculated	CVE-2018-20823 MISC MISC
zoho_manageengine -- adselfservice_plus	Zoho ManageEngine ADSelfService Plus before build 5708 has XSS via the mobile app API.	2019-04-24	not yet calculated	CVE-2019-11511 MISC
zotonic -- zotonic	Zotonic before version 0.47 has mod_admin XSS.	2019-04-24	not yet calculated	CVE-2019-11504 MISC
zyxel_communications -- multiple_devices	On Zyxel ATP200, ATP500, ATP800, USG20-VPN, USG20W-VPN, USG40, USG40W, USG60, USG60W, USG110, USG210, USG310, USG1100, USG1900, USG2200-VPN, ZyWALL 110, ZyWALL 310, ZyWALL 1100 devices, the security firewall login page is vulnerable to Reflected XSS via the unsanitized ‘mp_idx’ parameter.	2019-04-22	not yet calculated	CVE-2019-9955 MISC FULLDISC EXPLOIT-DB MISC CONFIRM